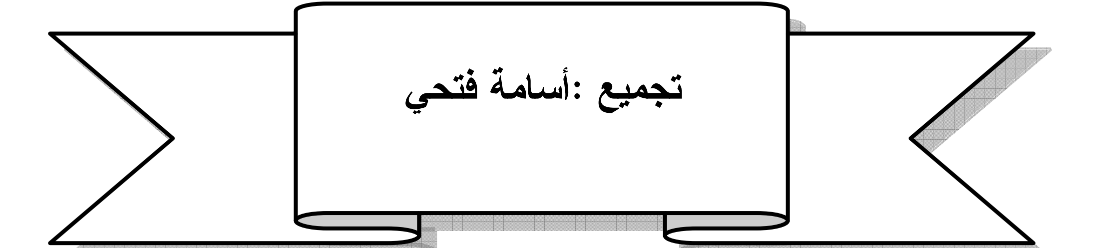
فيروسات الحاسب



المقـــــــــــــــدمــــــة

جرائم الحاسوب والانترنت

إن الاستخدام المتزايد للحاسبات والانترنت حقق أهدافا كثيرة لجميع المستخدمين وزاد من كفاءة الأعمال، إلا أن هناك مخاوف مستمرة من مخاطر الجرائم المختلفة المتعلقة بسرقة المعلومات والاحتيال وتدمير البيانات والإطلاع على خصوصيات الأفراد والمؤسسات والحكومات.

في هذا البحث سنتعرف على المفاهيم المتعلقة بتدمير البيانات ، وفيروسات الحواسيب المختلفة، وسنذكر الطرق المختلفة اللازمة للحذر والوقاية من هذه الأخطار التي لها آثار سلبية كبيرة ليست على الأفراد والمؤسسات فقط بل على المجتمع بشكل عام وسنلقي الضوء في هذا البحث أيضا على القواعد الأخلاقية العامة للتعامل مع الحاسبات.

بعض أنواع جرائم الحاسب

1. الاحتيال بالوصول إلى البيانات.
2. الاحتيال باستخدام بطاقات الائتمان.
3. نسخ البرامج.

الدوافع لارتكاب مختلف جرائم المعلوماتية فهي عديدة منها:

1. الرغبة في التفوق وتحدي التقنية المتطورة.
2. السعي إلى تحقيق مكاسب مالية والابتزاز.
3. دوافع سياسية وفكرية.
4. القيام بأعمال غير مشروعة
5. الأحقاد والدوافع الثأرية والانتقام من أرباب العمل.

جدول المحتويات

تعريف فيروس الـــحاسوب

الفيروس هو برنامج مكتوب بإحدى لغات البرمجة بواسطة أحد الـــمخربـــين بهدف إحداث الضرر بنظام الـــحاسوب. ويمثل فيروس الحاسوب نوعاً من أنواع جرائم التعدي على نظم الحاسبات.

الأسباب التي تدفع بعض الناس لكتابة البرامج الفيروسية

1 . الحد من نسخ البرامج كما في فيروس Pakistani أو brain
وهو أول فيروسات الكمبيوتر ظهورا و أكثرها انتشارا و كتب مـــن قبـــل اخـــوين مـــن الباكستان كحماية للملكية البرمجية للبرامج التي قاما بكتابتها .

2 . البحث العلمي كما في فيروس.STONED الشهير و الذي كتبة طالب دراسات عليـــا في نيوزيلندة و سرق من قبل أخيه الذي أراد أن يداعب أصدقاءه بنقل الفيروس إليهم .

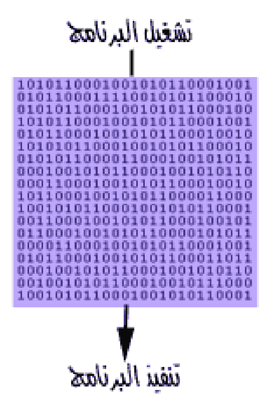
3 . الرغبة في التحدي و إبراز المقدرة الفكرية من بعض الأشخاص الذين يسخرون ذكاءهم و قدراتهم بشكل سيئ مثل فيروسات V2P

4 . التشجيع على شراء البرامج المضادة للفيروسات إذ تقوم بعض شركات البرمجة بنشر فيروسات جديدة ثم تعلن عن منتج جديد لكشفها .

كيف يعمل الفيروس ؟

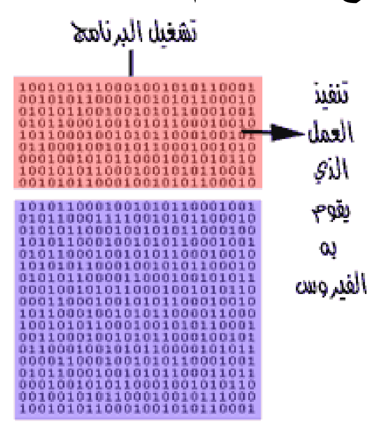
في الواقع يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بدايـــة أو نهايـــة الملـــف

المصاب، دون أن يقوم فعلياً بأي تغيير في مكوّنات الملف الأصلية. لننظر للصورة التاليــة التي توضّح شكل البرنامج غير المصاب بفيروس:

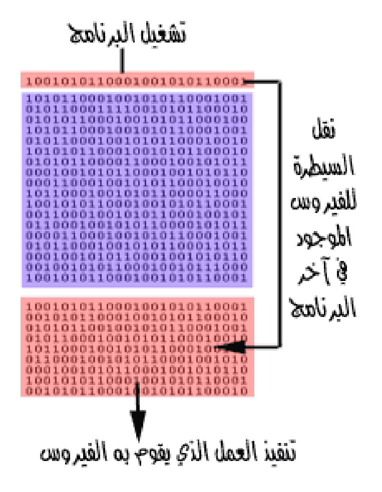


نلاحظ أنه عند استدعاء البرنامج فإنه يعمل بشكل طبيعي.

والآن لنتصوّر أنه تم إصابة البرنامج بفيروس. في الواقع يقوم الفيروس بلصق نفسه فــي البرنامج كما أسلفنا دون أن يغير في محتويات الملف شيئاً. و طريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه:



وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب، و يضع علامة في بدايته هكذا:



إن هذا الفيروس يختبئ في نهاية الملف المصاب، و يضع في مقدّمة البرنامج مؤشّراً بحيث أنه عندما يتم استدعاء البرنامج و تشغيله، يحوّل السيطرة للفيروس بدلاً من تشغيل البرنامج.

وفي الحالتين قد يعود الفيروس بعد الانتهاء من تنفيذ عمله المؤذي لتشغيل البرنامج و لكنه قد لا يعود أيضاً و يسبب أضراراً جسيمة للجهاز. ويحاول كل فيروس تقريباً أن يقوم بنفس الشيء.. وهو الانتقال من برنامج إلى آخر ونسخ الشفرة إلى الذاكرة ومن هناك تحاول الشفرة نسخ نفسها إلى أي برنامج يطلب العمل أو موجود بالفعل قيد العمل، كما تحاول هذه الشفرة أن تغير من محتويات الملفات ومن أسمائها أيضاً دون أن تعلم نظام التشغيل بالتغيير الذي حدث، مما يتسبب في فشل البرامج في العمل.

أشهر الفيروسات

. فيروس ساسر SASR

أصاب الفيروس ساسر في مايو 2004 أجهزة الحاسوب في العالم بنسبة 3.17% التي تعمل بنظام تشغيل ويندوز وذلك من خلال الانترنت ويسبب هذا الفيروس تأخيراً في تنفيذ الأوامر التي تعطى للجهاز كما يعمد إلى إغلاق الجهاز وإعادة فتحه.

فيروس جوبوت Gobot

نوع من الفيروسات التي تستغل الثغرات الأمنية التي توجد في نظام التشغيل ويندوز لكي ينفذ منها إلى الحاسبات التي يستهدفها، وينتشر هذا الفيروس من خلال الشبكات، ويقوم فور وصوله إلى الحاسوب بإيقاف عمل برامج مقاومة الفيروسات وبرامج التأمين الأخرى مثل برامج حائط النار Firewall كما يوقف عمل بعض الفيروسات الخطيرة على الحاسوب

مثل فيروس بلاستر Blaster، وقد يكون هذا نوعاً من التنـــافس بـــين صـــائغي بـــرامج الفيروس للحصول على السيطرة الكاملة على الحاسبات.

<u>. فيروس مايدوم</u>

نوع من الفيروس الذي يلحق برسالة البريد الإلكتروني كملف نصي ويقوم بإعادة إرســـال نفسه لعناوين إلكترونية أخرى إذا ما تم الإطلاع عليه، كما ينتـــشر مـــن خـــلال ملفـــات الموسيقى والأفلام والألعاب عبر الانترنت.

ويقوم الفيروس بإدخال برنامج يسمح للهاكرز المتطفلين والقراصنة بالدخول إلى جهـــازك وتسجيل كل ما تم طباعته ابتداء من كلمة السر إلى أرقام بطاقات الائتمان، وقد أصاب هذا الفيروس حوالي 500000 .

<u>melissa virus فيروس ميليسا</u>

هي من أسرع الفيروسات التي انتشرت في عام 1999 وهي متخصصة في إصابة البريد الإلكتروني و هي تقوم بالانتشار عن طريق الالتصاق في برامج النصوص كملحـــق فـــي رسالة البريد الالكتروني .

ما هو التروجان

تعريفة:

التروجان هو برنامج تجسس و له أسماء أخرى مثل مخدم server أو اللاصق parch أو الجاسوس spy لكن مبدعين هذا النوع من الملفات يفضلون الأسماء الرنانـــة و اســـم تروجان هو نسبة إلى حصان طروادة ، لكن مع اختلاف المسميات فهو برنـــامج تجســـسي يجعل من حاسبك مخدم لحاسب الجاسوس أي يتمكن الجاسوس من التحكم بجهازك و كأنـــة أنت لكن مع الأخذ بعين الاعتبار أن ذلك فقط في حال أنت متصل بالإنترنت أو الـــشبكة و ليس هذا فقط بل و عندما يعرف أنك على الإنترنت أما غير ذلك فهو لا حول له و لا قوة .

كيف يصل التروجان إلى الجهاز

1 . يرسل إليك عن طريق البريد الإلكتروني كملف ملحق فتقوم باستقباله وتشغيله وقـــد لا يرسل لوحده حيث من الممكن أن يكون ضمن برامج أو ملفات أخرى .

2 . إذا كنت من مستخدمي برنامج أي سي كيو .. أو بـــرامــــج التحادث فقد يرسل لـــك ملف مصاب بملف تجسس أو حتى فيروس .

3 .عـــندما تـــقـــوم بإنزال بـــرنامج من أحد المواقع الغير موثوق بها وهي كثيرة جدا فقد يكون البرنامج مـــصاباً بـــمـــلــــف تـــجسس أو فـــيـــــروس وغـــالـــبـــاً مـــــا يـــكـــون أمراً مقصوداً .

4 .طريـــقــــة أخـــرى لتحـــمـــيـــل تـــتـــلخـــص في مجرد كتابة كوده على الجهـــاز

نفسه في دقائق معدودة حيث أن حصان طروادة يــخــتــلــف عــن الفــيــروس في أنه مجرد برنامج ضئــيــل الحــجــم جــداً مــكــون فــقــط مــن عــدة أســطر قــلــيــلــة .

5 .أما لو كان جهازك متصل بشبكة داخــلية أو شبكة إنترانت .. فإنه في هذه الحالة يمكن نقل الملف الجاسوس من أي وحدة عمل فرعية .

6 .يــمــكــن نــقــل الملف أيضا عن طريق الإنترنــت بواســطة أي برنــامج FTP

7 . أخــيرا يمكن تخليق حصان طروادة من خلال إعادة تهيئة بعض البــرامج الموجــودة على الحــاسب مــثــل المــاكــروز المــوجــودة فــي بــرامــج مــعــالجــة الــنــصوص .

الوقاية من التروجان

استخدام برنامج مضاد للفيروسات حديث و قم بتحديثه باستمرار مع استخدام جدار نــاري جيد مثل (zone alarm) .
عدم تحميل أي برنامج مجاني مجهول المصدر و خاصة إذا كان من موقع شخصي أو من موقع مشبوه .
تجنب فتح الرسائل الإلكترونية ذات المصادر الغير معروفة خاصة تلك التي تحمل ملفــات مرفقة .
تعديل مستوى الأمن في المتصفح بحيث لا يتم قبول نزول أي برنامج من هذه البرامج إذا لم ترغب في منع هذه البرامج بشكل تام فيمكنك قبــول البــرامج التــي تحمــل التوقيــع الإلكتروني لمصدرها .

الدودة worm

هي تشبه الفيروسات والبعض يصنفها على أنها أحد تصنيفاته .... لها القدرة على الانتشار من جهاز إلى آخر ولكنها خلاف الفيروسات فهي لا تحتاج مساعده من أي شخص للانتقال فهي تستغل أي ملف يتم نقله من جهاز لآخر فيما يعرف بالانتقال غير المدعوم

الخطر الكبير للدودة هي القدرة على التكاثر والانتشار بكمية كبيرة

تشغل الذاكرة العشوائية للتكاثر والانتشار مما يؤثر على جهازك وأداؤه

لها القدرة على الانتشار عبر الشبكة.

الدودة صممت لكي تعمل كنفق أو مدخل إلى جهازك مما يسمح للهكر بالتحكم في جهـــازك عن بعد .

أشهر جرائم الدودة

أشهر حدث يخص هذه الديدان كان سنة 1988، حيث قام أحد الطـــلاب (.Robert T) من جامعة (Cornell) ببرمجة أحد البرامج القادرة على التنقل عبر شبكة الاتصال، بعد 8 ساعات من إطلاقه عبر الشبكة استطاع البرنامج إصابة آلاف الأجهزة وإعطـــاب العديـــد منها، كانت سرعة انتقال هذه الدودة عبر الشبكة جد هائلة مما استحال معه القضاء عليهـــا، هذا الانتشار تسبب في إعطاب الشبكة مما اضطرت معه NSA (Security National Agency) من إيقاف الاتصالات طيلة يوم كامل.

أشهر أنواع الدودة

<u>*:Autorun virus*</u>

وهو من أكثر الفيروسات انتشارا في الوقت الأخير و أكثرها إزعاجا للمستخدم فهو لا يؤثر على الكيان الصلب للجهاز أو الويندوز ولكنة يقوم ببعض الدعابات التي تضايق المستخدم ويعتبر هذا النوع من الفيروسات من نوع worm.

<u>طرق انتشار هذا الفيروس :</u>

ينتشر أساسا من خلال الوسائط النقالة MP3 , MP4, Flash Memory، ..... أو إذا ركبت hard disk في جهاز مصاب بالفيروس فانه ينتقل إليه.

<u>أنواع هذا الفيروس :</u>

هناك إصداران أساسيان من هذا الفيروس وهما :

النوع الأول يطلق عليه Win32.Perlovga Virus وملفاته الأساسية هي :

AutoRun .inf & host .exe & Copy .exe وهذا النوع لم يعد منتشر كثيرا.

النوع الثاني فيطلق عليه RavMon Virus ومن أشهر ملفاته AutoRun .inf & Ravmon.exe .

<u>أعراض الإصابة بهذا الفيروس :</u>

1- ممكن كل ما تفتح drive تخرج رسالة ERROR .

2- ممكن كل ما تفتح drive يفتحه في نافذة جديدة .

3- ممكن كل ما تفتح drive تخرج نافذة Open With .

4- ممكن يغير أسماء drives يخليها كلها Local Disk .

5 – إخفاء Folder options أو إبطال عملها .

علاج هذا الفيروس :

استخدام انتي فيروس جيد مثل كاسبر 7 أو كاسبر 8 ، نورتن ، مكافي 2007 ، ، نوود 32 ، نورتن .

مع العلم يجب التحديث المستمر لهذه البرامج وأنا أفضل الكاسبر إذا أجريت التحديثات له بشكل مستمر .

ولخطورة هذا الفيروس وجدت بعض البرامج التي تخصصت في إزالة هذا الفيروس مثل

NOD32 VBS[Butsur.A,B]-Fix

Perlovga Removal Tool

RavMon Removal Tool

طرق انتقال الدودة

طريقة عمل الديدان تطورت اليوم بتطور أدوات الاتصال وبرامج المحادثة الفورية، وذلك بواسطة رسائل تحمل الدودة (غالبا على شكل سكريبت أو ملف بامتداد exe) وتستطيع بمجرد تفعيلها من جمع كل العناوين الإلكترونية الموجودة بالجهاز وإرسال نفسها إليهم جميعا.

مثل دودة (I Love you)والتي انتشرت بسرعة هائلة عبر ملايين الأجهزة عبر العالم يوم 4 مايو 2000 ، مما جعل الأمريكيين يقدرون خسارة حجمها يناهز السبعة ملايين دولار (لكن لحسن حضهم كانت الخسارة أقل من ذلك).

ما الفرق بين الدودة و التروجان و الفيروس

الفيروس:

الفيروس يلحق نفسه ببرنامج أو ملف وينتشر من جهاز إلى جهاز مثـــل انتـــشار مـــرض الإنسان.

في كل جهاز يدخله الفيروس يخلف وراءه العدو. خطر الفيروسات يختلف من نـــوع إلـــى آخر بعضها قد يؤدي إلى بعض الأعطال البسيطة وبعضها قد يسبب تلف الكيان الـــصلب أو البرامج لديك وحتى ملفاتك المهمة.

في العادة معظم الفيروسات تأتي على شكل ملف تنفيذي exe وهذه الملفات عند نزولها في جهازك لن تعمل حتى تقوم أنت بمحاولة تشغيلها، وللمعلومة الفيروسات لا تنتقل ذاتيا وإنما عن طريق الإنسان وذلك عندما يحاول تشغيلها أو إرسالها عن طريق الإيميل وهو لا يعلـــم بأنها تحتوي فيروسا.

ولكي تحمي نفسك من الفيروسات تحتاج إلى برنامج مكافحة الفيروسات وهو يعمـــل مثـــل المضاد الحيوي للإنسان فهذا البرنامج يقوم بزيادة مناعة جهازك ضد الفيروسات وبذلك تقل فرص إصابتك بهذه البرمجيات الخبيثة.

الدودة

الدودة قريبة من الفيروس في التصميم ولكن تعتبر جزءاً فرعياً من الفيـــروس .الاخـــتلاف الذي يفرق الفيروس عن الدودة بأن الدودة تنتشر بدون التدخل البشري حيث تنتقـــل مـــن جهاز إلى آخر بدون عمل أي إجراء.

الجزء الخبيث في الدودة هو قدرتها على نسخ نفسها في جهازك بعدة أشكال وبذالك يتم إرسالها بدلا من مرة وحدة سترسل آلافاً من النسخ للأجهزة الأخرى، مما يحدث مشاكل كبيرة وتستغل الدودة طرق الاتصال التي تقوم بها لإتمام هذه العملية لذالك قد ترى في بعض الأحيان ظهور نافذة طلب الاتصال اتوماتيكيا بدون طلبك أنت فانتبه فقد يكون لديك دودة.

وآثار الدودة عادة هي زيادة في استخدام مصادر الجهاز فيحصل في الجهاز تعليق بسبب قله الرام المتوفر وأيضا تسبب الدودة في توقف عمل الخوادم فعلى سبيل المثال يمكنك تخيل التالي: لو كان عندك دودة فستقوم الدودة بنسخ نفسها ثم إرسال نفسها لكل شخص من هم لديك في القائمة البريدية نسخة وإذا فتح احدهم هذه الرسالة ستنتقل إلى كل من لديه هو في قائمته البريدية وهذا يولد انتشاراً واسعاً جداً.

وأفضل مثال على الدودة هي ما حصل العام الماضي دودة البلاستر التي كانت تدخل لجهازك لتسمح لبعض الأشخاص بالتحكم بجهازك عن بعد .

التروجان:

التروجان يختلف كليا عن الفيروس والدودة . التروجان صمم لكي يكون مزعجاً أكثر من كونه مؤذياً مثل الفيروسات.

عندما تقوم بزيارة احد المواقع المشبوهة أحيانا يطلب منك تحميل برنامج معين. الزائر قد ينخدع في ذلك فيعتقد انه برنامج وهو في الحقيقة تروجان.

يقوم التروجان في بعض الأحيان بمسح بعض الأيقونات على سطح المكتب. مسح بعض ملفات النظام. مسح بعض بياناتك المهمة. تغير الصفحة الرئيسية للإنترنت إكسبلورر. عدم قدرتك على تصفح الانترنت. وأيضا عرف عن التروجان أنها تقوم بوضع(back door) في جهازك مما يسمح بنقل بياناتك الخاصة إلى الطرف الآخر بدون علمك.

وهذا هو الخطير في الأمر. علما بأن التروجان لا يتكاثر مثل الـــدودة ولا يلحـــق نفـــسه ببرنامج مثل الفيروس ولا ينتشر أيضا سواء عن تدخل بشري .

كيف نحمي أنفسنا من الفيروسات

للحيطة و الحذر من الفيروسات خاصة إذا كنت معتاداً على تبادل الأقـــراص المرنـــة، أو الملفات عبر الانترنت لابد من اتخاذ الخطوات التالية:

- لابد من موجود برنامج حماية من الفيروسات في جهازك.
- لابد أن تقوم بتحديثه بشكل دوري، وإلا فلا فائدة من وجوده.
- لا تقم بفتح المرفقات في أي إيميل لا تعرف مرسله.
- لا تقم بفتح المرفقات في إيميلات أصدقائك إذا وجدتها تنتهي بـــــ exe أو bat أو أي امتداد لا تعرفه.
- لا تقبل ملف من شخص لا تعرفه أبداً.
- إذا قبلت ملفاً من شخص تعرفه، افحصه أيضاً ببرنامج الحماية، فقد يكون صـــديقك نفسه ضحية.
- احرص على فحص جميع البرامج التي تقوم بتنزيلها من الإنترنت، أو تشغيلها مـــن قرص مرن أو سي دي. قبل أن تشغّلها.

لا تدخل إلى مواقع الهاكرز المنتشرة خاصةً إذا كنت غير متمكن ولم تتخـــذ الاحتياطـــات اللازمة، فبعضها ينسخ الفيروس مع الملفات المؤقتة. و لتجنّب مثل هذه الحـــالات يمكنـــك تفعيل خيار الحماية في التصفّح في برنامج الحماية الذي يقدّم مثل هذه الخدمة.

أخلاقيات الحاسوب والانترنت

أصدرت العديد من دول العالم المتقدم لوائح تشريعية لحماية خصوصية الأفـراد وهنـاك العديد من الأخلاقيات يجب على مستخدم الحاسوب التحلي بها وقد ذكرت إحدى الجمعيات التطوعية ذات النفع العام هذه الأخلاقيات نورد بعضها فيما يلي:

1. تجنب الإساءة للآخرين (التجسس، إرسال الفيروسات، توزيع الملفات غير الأخلاقية على الآخرين).
2. الإخلاص في العمل وعدم الانحياز في الأفكار.
3. احترام أملاك الآخرين وحقوق الملكية الفكرية.
4. احترام أفكار ومعتقدات الآخرين.
5. الالتزام بالسرية والتعهدات والاتفاقيات وقوانين العمل.

6 – بذل الجهد لتحقيق الأفضل، والأكثر فاعلية.

7. احترام خصوصية الآخرين.
8. تقبل النقد المهني، وانقد عمل غيرك بموضوعية.
9. المساهمة بتطوير الوعي الحاسوبي العام.
10. استخدام الحاسبات ونظمها حين يكون مسموحاً بذلك.